Cryptography & Security Research Project Proposal

Chi Yin Wong 836872

1. Introduction

The advancement of technology and improvement in engineering has resulted in a time where large scale quantum computers are no longer a dream, but a fast-approaching reality. These powerful computers will be sufficiently strong enough to solve difficult mathematical problems – many of which serve as the bedrock of current public key cryptographic algorithms. This means that although current cryptographic schemes such as RSA and Diffie Hellman are safe against modern technology, there is a motivation to develop more advanced algorithms that are secure enough to withstand the power of a quantum computer. This gives rise to the field of post-quantum cryptography, a field dedicated to exploring more advanced algorithms that are resistant against attacks from quantum computers, as well as improving existing hard mathematical-based schemes, preparing us for an era where quantum computers will be the norm [1].

2. Background

2.1 Public Key Encryption Schemes

Many public key cryptographic schemes are based on mathematical problems that are considered hard by today's computing standards. These schemes have been employed for a long period of time and have successfully prevented attacks. One such scheme is known as RSA, an algorithm used for both key exchange and digital signatures [2]. It is based on two key mathematical problems: integer factorization and finding the eth root mod n. Another popular scheme that is used often for key exchange is the Diffie-Hellman protocol. This protocol is based on the discrete logarithm problem, allowing two parties to communicate by creating a shared secret key without revealing their own private key [3].

2.2 Quantum Computers

Quantum computers are machines that employ the full complexity of the properties of quantum physics to store data and perform computations [4]. Rather than encode information in binary bits today's computers, quantum computers use quantum bits, bits made up of physical systems that can exhibit the property of quantum superposition. Quantum entanglement also allows quantum bits to be linked together [5]. Given a large number of possible combinations such as in hard mathematical problems like integer factorization, quantum computers can consider many computations simultaneously, solving these problems at a much faster rate [6].

2.3 Shor's Algorithm

Shor's algorithm is a polynomial time quantum algorithm designed to find the prime factorization of any large positive integer n [1]. It has a complexity of $O((\log(n))^2 * \log(log(n)))$ which is much faster than the complexity of classical computers which require exponential time [8]. A quick and very brief overview of Shor's algorithm is as follows. The

initial steps of Shor's algorithm include first determining if the integer n is prime, picking an integer q that satisfies $n^2 \leq q < 2n^2$ and picking an integer x that is co-prime to N. Then a quantum computer is used to create a partitioned quantum register with one register having enough quantum bits to represent integers as large as q-1 and the other to represent n-1. Register one will be loaded with an equally weighted superposition of integers from 0 to q-1 and register 2 will be loaded in the 0 state. A transformation of $x^a mod\ n$ (where a is the superposition of the states) is applied to every integer stored in register one and the result is stored in register two. A discrete Fourier transform is computed on register one and a value m which is the state of register one will have a very high probability of being a multiple of q/r where r is unknown and can be found with post processing techniques on classical computers based on knowing m and q. A factor of n can be found by taking the greatest common divisor of $x^{r/2} \pm 1$ and n [7].

3. References

[1] DJ. Bernstein, T. Lange. "Post-quantum cryptography" in Nature, vol. 549, pp. 188-194, 2017.

[2] NY. Goshwe. "Data Encryption and Decryption Using RSA Algorithm in a Network Environment" in IJCSNS International Journal of Computer Science and Network Security, vol. 13, no. 7, pp. 8-13, 2013.

[3] UM. Maurer, S. Wolf. "The Diffie-Hellman Protocol" in Designs, Codes and Cryptography, vol. 19, pp. 147-171, 2000.

[4] TD. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monnroe, JL. O'Brien. "Quantum Computers" in Nature, vol. 464, pp. 45-53, 2010.

[5] OH. Montiel Ross, "A Review of Quantum-Inspired Metaheuristics: Going From Classical Computers to Real Quantum Computers" in IEEE Access, vol. 8, pp. 814-838, 2020.

[6] KA. Valiev. "Quantum computers and quantum computations" in Physics-Uspekhi, vol. 48, pp.1, 2005.

[7] M. Hayward. "Quantum Computing and Shor's Algorithm". Sydney: Macquarie University Mathematics, 2008.

[8] MJ. Nene, G. Upadhyay. "Shor's Algorithm for Quantum Factoring" in Advanced Computing and Communication Technologies. Advances in Intelligent Systems and Computing, vol. 452, pp. 325-331, 2016.